SECURITY AND PRIVACY PROTECTION METHOD FOR ELECTRONIC PATIENT'S CHART

Patent Number: JP2000348123
Publication date: 2000-12-15
Inventor(s): YOSHIDA AKIRA
Applicant(s): YOSHIDA AKIRA
Requested Patent: ☐ JP2000348123
Application Number: JP19990162258 19990609
Priority Number(s):
IPC Classification: G06F19/00; G06F17/60
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To realize security and privacy protection for electronic patient's chart which surely prevent alteration of an electronic patient's chart and certify that a patient has been explained to and has consented in the case of the occurrence of a matter of explanation and consent.
SOLUTION: The consent of a patient or his family can be inputted to the electronic patient's chart with characters or a voice besides medical treatment contents, and the ID of a doctor or an input person and a time stamp are inputted also. A system device of a medical institution receives delivery of a time stamp from a reliable institution and sends into the electronic patient's chart to write it and sends contents of the electronic patient's chart and consent item contents to the reliable institution together with the time stamp, and the reliable institution stores and preserves contents of the electronic patient's chart and the time stamp together with delivery of the time stamp and the ID of the medical institution and prints them to obtain a settlement date from a notary public. These contents are produced based on a court order to produce, and contents of the electronic patient's chart are confirmed to prevent alteration of the electronic patient's chart and to protect privacy.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－348123
（P2000－348123A）
(43)公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/42	Ｈ	５Ｂ０４９
17/60		15/21	３６０	

審査請求　未請求　請求項の数４　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－162258

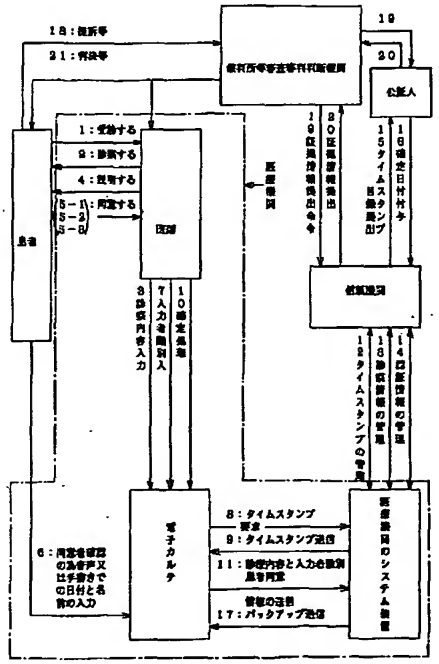
(22)出願日　平成11年６月９日(1999.6.9)

(71)出願人　596021399
吉田　彬
長崎県佐世保市権常寺町405番地８
(72)発明者　吉田　彬
長崎県佐世保市権常寺町405番地８
(74)代理人　100081824
弁理士　戸島　省四郎

Ｆターム(参考)　5B049 AA05 BB42 DD00 DD01 DD03
DD05 EE05 FF09 GG02 GG04
GG07 GG10

(54)【発明の名称】　電子カルテにおけるセキュリティ確保とプライバシー保護方法

(57)【要約】
【課題】　電子カルテの改ざんを確実に防ぎ、患者への説明と同意が後で問題となったときにそれを証明できる電子カルテのセキュリティ確保とプライバシー保護を実現する。
【解決手段】　電子カルテに診療内容の他に患者又は家族からの同意を文字による入力又は音声による入力を可能とし、又医師・入力者のＩＤ及びタイムスタンプを入力する。又医療機関のシステム装置は、信頼機関からタイムスタンプの交付を受け、電子カルテに送り込んで書き込み、又電子カルテの内容・同意事項内容をタイムスタンプとともに信頼機関に送り、信頼機関はタイムスタンプの交付と医療機関のＩＤとともに電子カルテ内容・タイムスタンプを記憶保存し、これらを印刷して公証人から確定日付をもらう。これらの内容は裁判所の提出命令に基づいて提出して、電子カルテの内容の確認によって電子カルテの改ざんを防止し、又プライバシーを保護できるようにする。



【特許請求の範囲】
【請求項１】　通信される通信内容のデータと通信日時を記録保管し、タイムスタンプを発行管理し、データと通信日時の機密を保持する信頼機関を設け、
医師が作成する電子カルテの内容・情報を記憶保存し、その内容・情報を前記信頼機関に送るとともに信頼機関からタイムスタンプの交付を受け、同タイムスタンプを医師が作成する電子カルテに付加させる医療機関のシステム装置を設け、
医療機関の医師は、コンピュータと電子記録媒体とによって作成される電子カルテの新規作成、カルテの追加、変更、削除事項の際、必要に応じ患者に診療内容を説明し、閲覧可能な職種、第三者及び閲覧可能な内容について、音声又は手書きで日時と氏名そして同意内容を患者又はその家族等に入力をもとめ、更に必要に応じ医師の音声又は手書きでの確認を電子カルテに入力し、当該入力内容を必要に応じ医師のパスワード入力とともに電子カルテ内容に付加し必要に応じ医療機関のシステム装置を介して前記信頼機関から日時のタイムスタンプを取得し、タイムスタンプをそれまで得られた内容に付加し、当該データを医療機関のシステム装置を介して信頼機関におくり、
信頼機関は各医療機関、各患者毎の当該タイムスタンプ目録を作成し印刷したものとデータを蓄積した媒体に対して定期的に公証人確定日付をもらい保管し、電子カルテの内容、日付の存在と同一性の判断をする時点で信頼機関に蓄積した確定日付番号付き目録又は電子媒体を裁判所所属又は委託を受けた有資格者の立会の下で開封してその電子カルテの内容を確認し、その後コピーして再度密封し、該確認行為を表示する確定日付番号を刻印して証拠性の維持を計るようにする一方、定期的に蓄積した確定日付番号付き媒体中のデータから当該データ相当データを検索し、双方照らし合わせ改ざんの有無を検査し、又、患者情報の不当な流通、権限なき又は同意なき閲覧がないか調査し、電子カルテにおけるセキュリティ確保とプライバシー保護を実現する方法。
【請求項２】　信頼機関は、医療機関に対して暗号化したタイムスタンプを送信して交付し、医療機関のシステム装置は電子カルテの入力者に対して暗号化したタイムスタンプを電子カルテに付加して書き込み、信頼機関と医療機関のシステム装置は上記暗号化したタイムスタンプを記憶・管理する請求項１記載の電子カルテにおけるセキュリティ確保とプライバシー保護方法。
【請求項３】　信頼機関は、公開鍵暗号方式を使用したタイムスタンプを医療機関のシステム装置へ送り、医療機関のシステム装置は入力者が作成する電子カルテに書き込み、信頼機関と医療機関のシステム装置はそのタイムスタンプ・公開鍵を記憶・管理する請求項１記載の電子カルテにおけるセキュリティ確保とプライバシー保護方法。
【請求項４】　電子カルテに付加する医師のパスワードの他に、入力者の識別の情報を手書サイン又は音声で入力するものである請求項１～３何れか記載の電子カルテにおけるセキュリティ確保とプライバシー保護方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、病院・医院・治療機関等医療機関で作成するコンピュータを用いて電子媒体に記録される電子カルテの改ざん防止するセキュリティ確保とプライバシー保護を実現する方法に関する。
【０００２】
【従来の技術】従来の医療機関のカルテは医師が紙に記入する方法が一般的であったが、今日コンピュータ化に伴ってカルテ内容をコンピュータのＦＤ・ＭＯ・ＨＤ・光ディスク・磁気テープ・ＩＣメモリ等の記憶媒体に記憶して電子カルテとし、その呼び出し・検索・照合を容易にして使い易くする方向にある。しかしながら、カルテは改ざんすることが許されていず、又改ざんがないように保管し、又改ざんがあればそれを検証できることが必要とされている。電子カルテは技術的には改ざんが容易であり、且つその改ざんの立証がきわめて難しいものとなりがちであった。
【０００３】
【発明が解決しようとする課題】本発明が解決しようとする課題は、従来のこれらの問題点を解消し、電子カルテの改ざんを確実に防ぐことができ、しかも、患者への説明と同意が後で問題になったときにそれを証明できる電子カルテのセキュリティ確保とプライバシー保護を実現する方法を提供することにある。
【０００４】
【課題を解決するための手段】かかる課題を解決した本発明の構成は、
１）　通信される通信内容のデータと通信日時を記録保管し、タイムスタンプを発行管理し、データと通信日時の機密を保持する信頼機関を設け、医師が作成する電子カルテの内容・情報を記憶保存し、その内容・情報を前記信頼機関に送るとともに信頼機関からタイムスタンプの交付を受け、同タイムスタンプを医師が作成する電子カルテに付加させる医療機関のシステム装置を設け、医療機関の医師は、コンピュータと電子記録媒体とによって作成される電子カルテの新規作成、カルテの追加、変更、削除事項の際、必要に応じ患者に診療内容を説明し、閲覧可能な職種、第三者及び閲覧可能な内容について、音声又は手書きで日時と氏名そして同意内容を患者又はその家族等に入力をもとめ、更に必要に応じ医師の音声又は手書きでの確認を電子カルテに入力し、当該入力内容を必要に応じ医師のパスワード入力とともに電子カルテ内容に付加し必要に応じ医療機関のシステム装置を介して前記信頼機関から日時のタイムスタンプを取得し、タイムスタンプをそれまで得られた内容に付加し、

当該データを医療機関のシステム装置を介して信頼機関におくり、信頼機関は各医療機関、各患者毎の当該タイムスタンプ目録を作成し印刷したものとデータを蓄積した媒体に対して定期的に公証人確定日付をもらい保管し、電子カルテの内容、日付の存在と同一性の判断をする時点で信頼機関に蓄積した確定日付番号付き目録又は電子媒体を裁判所所属又は委託を受けた有資格者の立会の下で開封してその電子カルテの内容を確認し、その後コピーして再度密封し、該確認行為を表示する確定日付番号を刻印して証拠性の維持を計るようにする一方、定期的に蓄積した確定日付番号付き媒体中のデータから当該データ相当データを検索し、双方照らし合わせ改ざんの有無を検査し、又、患者情報の不当な流通、権限なき又は同意なき閲覧がないか調査し、電子カルテにおけるセキュリティ確保とプライバシー保護を実現する方法

2) 信頼機関は、医療機関に対して暗号化したタイムスタンプを送信して交付し、医療機関のシステム装置は電子カルテの入力者に対して暗号化したタイムスタンプを電子カルテに付加して書き込み、信頼機関と医療機関のシステム装置は上記暗号化したタイムスタンプを記憶・管理する前記1）記載の電子カルテにおけるセキュリティ確保とプライバシー保護方法

3) 信頼機関は、公開鍵暗号方式を使用したタイムスタンプを医療機関のシステム装置へ送り、医療機関のシステム装置は入力者が作成する電子カルテに書き込み、信頼機関と医療機関のシステム装置はそのタイムスタンプ・公開鍵を記憶・管理する前記1）記載の電子カルテにおけるセキュリティ確保とプライバシー保護方法

4) 電子カルテに付加する医師のパスワードの他に、入力者の識別の情報を手書サイン又は音声で入力するものである前記1）～3）何れか記載の電子カルテにおけるセキュリティ確保とプライバシー保護方法にある。

【0005】

【発明の実施の形態】本発明の電子カルテは医療機関のコンピュータとその通信回線（LAN又は電話回線・専用回線）を用いて医師の仕事場の近くに設置したコンピュータ端末装置でキーボード・マウスによる入力・管理・表示できるようにする。及び手書き文字の入力装置（スキャナー入力，パッド入力）・音声（マイク入力）入力装置・デジタルカメラ等を備える医療機関は中央に

・説明内容提示
・開示相手
・機関
・職種

同意を得られなければ処理ステップ7，8へ移行する。

ステップ5－2：医師は患者又はその家族に診察内容等の説明を行い、カルテを閲覧してもよい第三者（機関　職種　特定者）と閲覧してよい内容（医師診察所見、検査、処方、病名等）を説明する。

これらのシステム管理・記憶・管理・通信を行うコンピュータを用いたシステム装置を設置し、病院に電子カルテ作成・表示可能なコンピュータ端末装置を多数設ける。信頼機関には、同様に通信機能を有するコンピュータ装置を設置し、データ内容・通信内容・時間・通信相手等を記憶・保管・更新し、印刷を行い、又タイムスタンプを発生しそれを通信回線を介して医療機関・医師・患者毎程に交付し、管理する。医療機関のシステム装置と信頼機関は通信可能で互にデータを高速でやりとりできるようにする。コンピュータ端末装置・医療機関のシステム装置・信頼機関のコンピュータ装置には、通常の通り、CPU，ROM，RAM，大量記憶媒体としてのHD，MO，光ディスク，磁気テープ，プリンター，キーボード，マウス，ディスプレイ，ISDN又はモデムの通信機器，有線・無線の通信ライン等の装置を備えてあり、CPUにはこれらの管理システムソフト，電子カルテ作成ソフト，通信ソフト，記憶保管システムソフト等が作動できるようになっている。

【0006】

【実施例】以下、本発明の実施例を図面に基づいて説明する。図1は、実施例を示す説明図である。図2は、実施例の電子カルテ作成の行程説明図である。図3は、実施例の医療機関のシステム装置と信頼機関との通信・処理のフローを示す説明図である。図4は、実施例の処理フローの内容を示す説明図である。図5は、実施例の電子カルテの真正性の説明図である。

A：診療と電子カルテ処理の流れ（図1，4参照）

医師が電子カルテの確定処理するまでの処理は下記のステップの通りになされる。

ステップ1：患者は受診する。

ステップ2：医師は診察する。医師又は入力者は電子カルテの頭書を入力・変更又は確認する。

ステップ3：医師は電子カルテにその診療結果・検査・処方・病名等を入力する。

ステップ4：診療結果・検査・処方・病名を患者に説明する。

ステップ5－1：プライバシー保護のためアクセス権を設定し、必要に応じて患者又はその家族等から下記の項目に関しインフォームドコンセントを得られるか否か。

・特定者
・開示内容
・医師診察内容
・検査
・処方

ステップ5－3：患者又は、その家族はカルテを第三者に閲覧されることを同意したか？説明し了解してもらった内容の確認を得る。同意を得られなければ処理ステップ7，8へ移行する。

ステップ6：年月日時と患者（又はID）又は家族等の

名前を音声又は手書きで当該者に電子記録（患者サイン情報とする）してもらう。これはマイク入力，パッド入力，スキャナー入力，デジタルカメラ等によって画像又は音声を入力可能とする。前記ステップ５－１，５－２，５－３，６の行程によって、病名等を説明し了解してもらった内容の確認を得その証拠として必要に応じて年月日と患者（又名前はＩＤ）又は家族等の名前を音声又は手書きで該当者に表示してもらい電子記録（患者サイン情報とする）する確定処理を行う。これによってセキュリティとプライバシーを確保する。

ステップ７：入力責任者は識別情報としてパスワードだけでよいかシステム装置に尋ねる。

・ＹＥＳの場合

入力者はパスワードのみ入力する。

・ＮＯの場合

入力者はパスワード入力の他に下記のものも入力する。

・手書きをもとめる

年月日時と診察者又は入力者の名前（又はＩＤ）を手書きで当該者に記録（入力者サイン情報とする）してもらう。

・音声をもとめる

年月日時と診察者又は入力者の名前（又はＩＤ）を音声で当該者に記録（入力者サイン情報とする）してもらう。

ステップ８：入力者は医療機関のシステム装置に対してタイムスタンプを要求する。不要であればステップ１０へ

ステップ９：医療機関は入力者対策のレベルが下記のいずれかであるか問い合わせる。その回答のレベルに応じた下記のタイムスタンプ処理を行う。

・軽度の対策の場合

信頼機関へ暗号化しないタイムスタンプの送信をもとめる。

・中程度の対策の場合

信頼機関へ共通鍵で暗号化したタイムスタンプの送信をもとめる。

・高度の対策の場合

信頼機関へ公開鍵暗号方式を使用したタイムスタンプの送信をもとめる。次に信頼機関は自身の秘密鍵で信頼機関名又はＩＤを暗号化し、医療機関のシステム装置へタイムスタンプを送信し、システム装置はタイムスタンプを入力者に送り、電子カルテに書き込む。信頼機関はそのタイムスタンプを医療機関・医師・患者ＩＤ・時刻を記憶保存する。

ステップ１０：入力者は確定処理を行い、電子カルテ書き込み・保存を完了する。

・医療機関のシステム装置はタイムスタンプを受信し、自身の秘密鍵でタイムスタンプを複号化し、必要に応じ医療機関のシステム装置は上記内容を独自の共通鍵で暗号化し共通鍵を医療機関で管理する。必要に応じ当該共通鍵を信頼機関のシステム装置の公開鍵で暗号化する。

ステップ１１：電子カルテの内容，入力者の識別，患者の同意の内容を医療機関のシステム装置へ送信する。

ステップ１２：医療機関のシステム装置は電子カルテのカルテ内容とタイムスタンプを信頼機関に送信する。

ステップ１３：信頼機関は送信された情報を医療機関毎に特定し保存する。

ステップ１４：信頼機関は認証情報の管理を行う。

ステップ１５：信頼機関は送信したタイムスタンプの目録を毎日又は一定の周期で印刷する。

ステップ１６：印刷された目録を公証人によって確定日付をもらう。これによって、セキュリティの確保とプライバシー保護を実現する。目録は医療機関毎に、当該医療機関に発行した医療機関毎連番を振ったタイムスタンプと患者ＩＤ、診察者ＩＤより構成される。

ステップ１７：医師は、医療機関のシステム装置から情報を受け取り、又必要に応じてバックアップ送信を受ける。

ステップ１８：患者が電子カルテ関係の医療事案で提訴する。

ステップ１９：裁判所は信頼機関・公証人へ証拠・情報提出命令を発する。

ステップ２０：信頼機関・公証人は、保存している証拠・情報を裁判所へ提出する。

ステップ２１：裁判所は電子カルテの内容について、信頼機関・公証人の提出証拠・情報提供資料に基づいて判断・判決する。

以上のシステムによって、電子カルテの改ざんは困難となり、仮に改ざんがなされれば確実にその改ざんが判定でき、且つ立証できるものとなる。又個人のプライバシーも同意の明確さ、又その立証の確実さとコンピュータ・電子カルテへのアクセスが難しいことから充分に保護される。

Ｂ．医療機関でデータ破損又は消失が生じたとき（図４（Ｃ）参照）

信頼機関は医療機関毎に保存した当該データをコピーし返送することで回復できる。

Ｃ．診察、患者への説明、監査、訴訟等で医療機関でデータの真正性を証明する必要が生じたとき（図４（ｄ）参照）

信頼機関は医療機関毎に保存した当該データをコピーし正当な理由と権利又は権限をゆうする個人又は機関に証拠物件として提出し、医療機関提出資料のデータと相違のないことをもって真正性を証明する。

Ｄ．信頼機関のデータの真正性は公証人が付与した確定日付付きタイムスタンプ目録により担保される（図１の行程１５，１６参照）。

Ｅ．プライバシー保護

下記プライバシー保護及び改ざんからのセキュリティは上記システムによって下記の点が保護されている。

・漏洩対策・アクセス権設定・情報の真正性・改ざん対策・虚偽入力・記録の共同責任者や責任の有る人による後からの更新履歴の保存、書換、消去、混同

Ｆ．作成の責任の所在

責任のないひとが責任の有るひとに成りすまして入力、代行入力者の存在は　　作成責任者や入力者の識別（ＩＤ，パスワード等）によってチェック・防止できる。

Ｇ．見続性

電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできる。

【０００７】

【発明の効果】以上の様に、本発明によれば患者のプライバシーが保護されながら、電子カルテの改ざんができず、又電子カルテの機密を保持しての保存が行え、又電子カルテの回復も容易で証拠力も高いものにできる。

【図面の簡単な説明】

【図１】実施例を示す説明図である。

【図２】実施例の電子カルテ作成の行程説明図である。

【図３】実施例の医療機関のシステム装置と信頼機関との通信・処理のフローを示す説明図である。

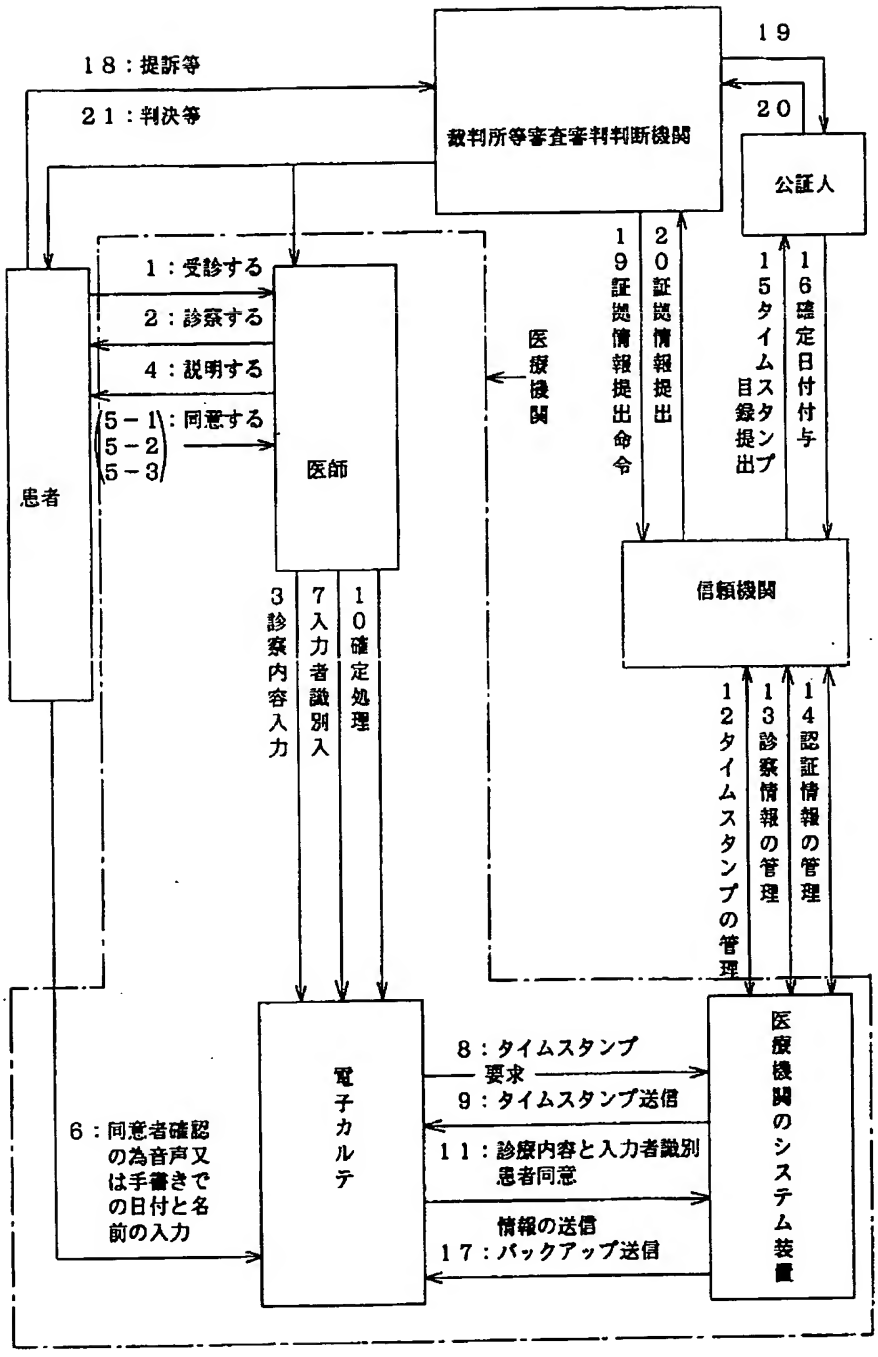
【図４】実施例の処理フローの内容を示す説明図である。

【図５】実施例の電子カルテの真正性の説明図である。

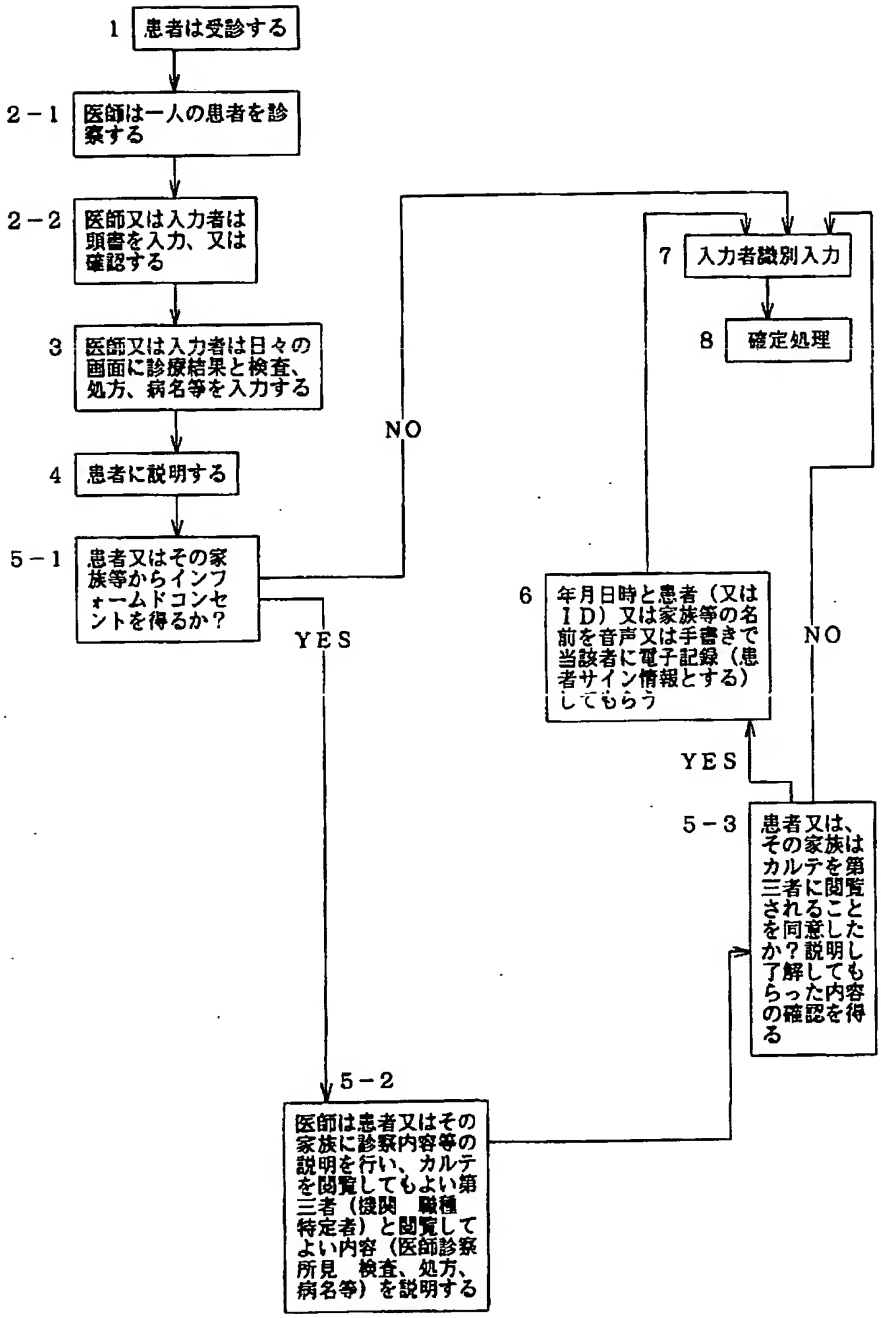
【符号の説明】

１～２１　処理のステップ

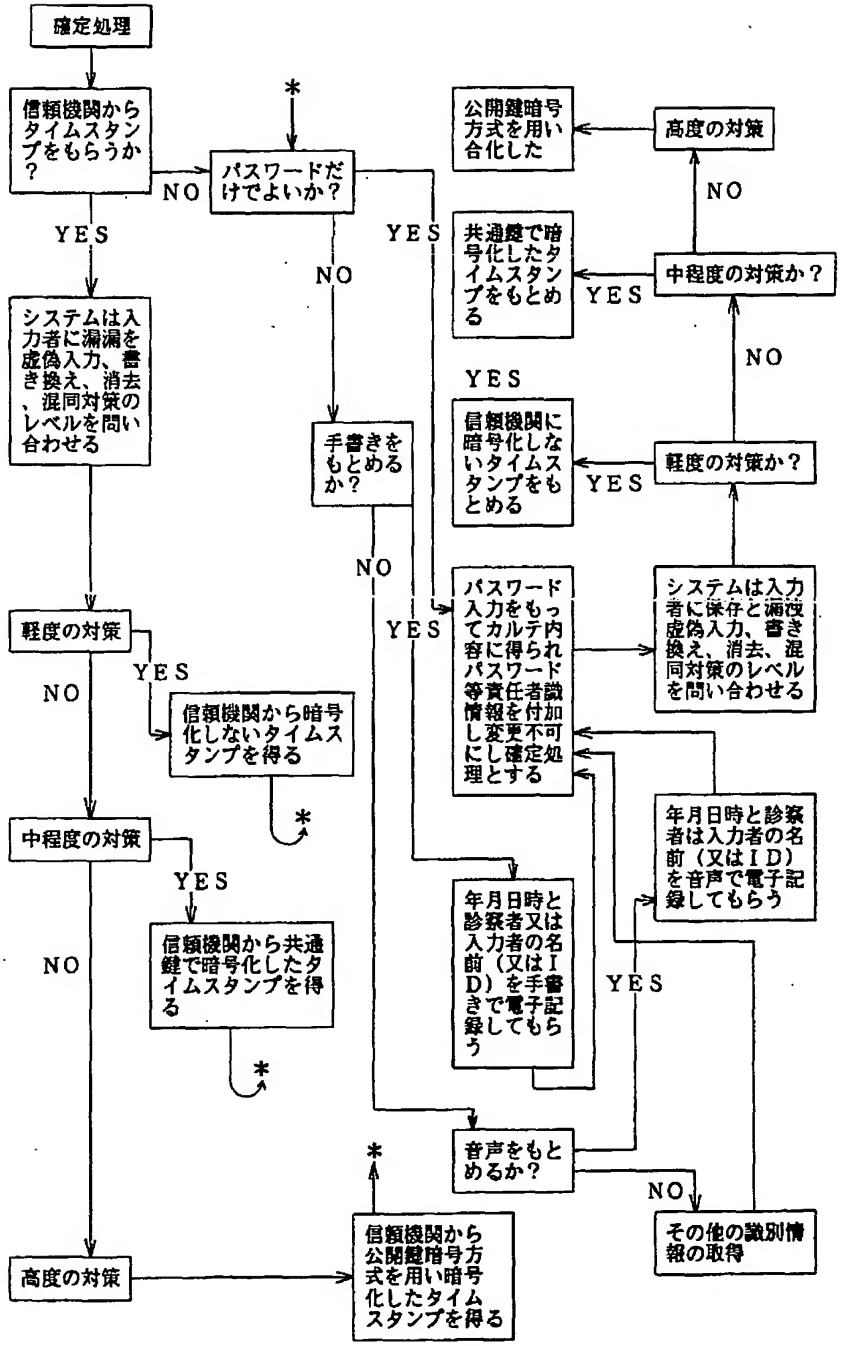
【図1】


裁判所等審査審判判断機関
公証人
信頼機関
医師
患者
医療機関
電子カルテ
医療機関のシステム装置
18：提訴等
21：判決等
19
20
1：受診する
2：診察する
4：説明する
5－1
5－2
5－3
：同意する
19証拠情報提出命令
20証拠情報提出
15タイムスタンプ目録提出
16確定日付付与
3診察内容入力
7入力者識別入
10確定処理
12タイムスタンプの管理
13診察情報の管理
14認証情報の管理
8：タイムスタンプ要求
9：タイムスタンプ送信
11：診察内容と入力者識別患者同意
情報の送信
17：バックアップ送信
6：同意者確認の為音声又は手書きでの日付と名前の入力

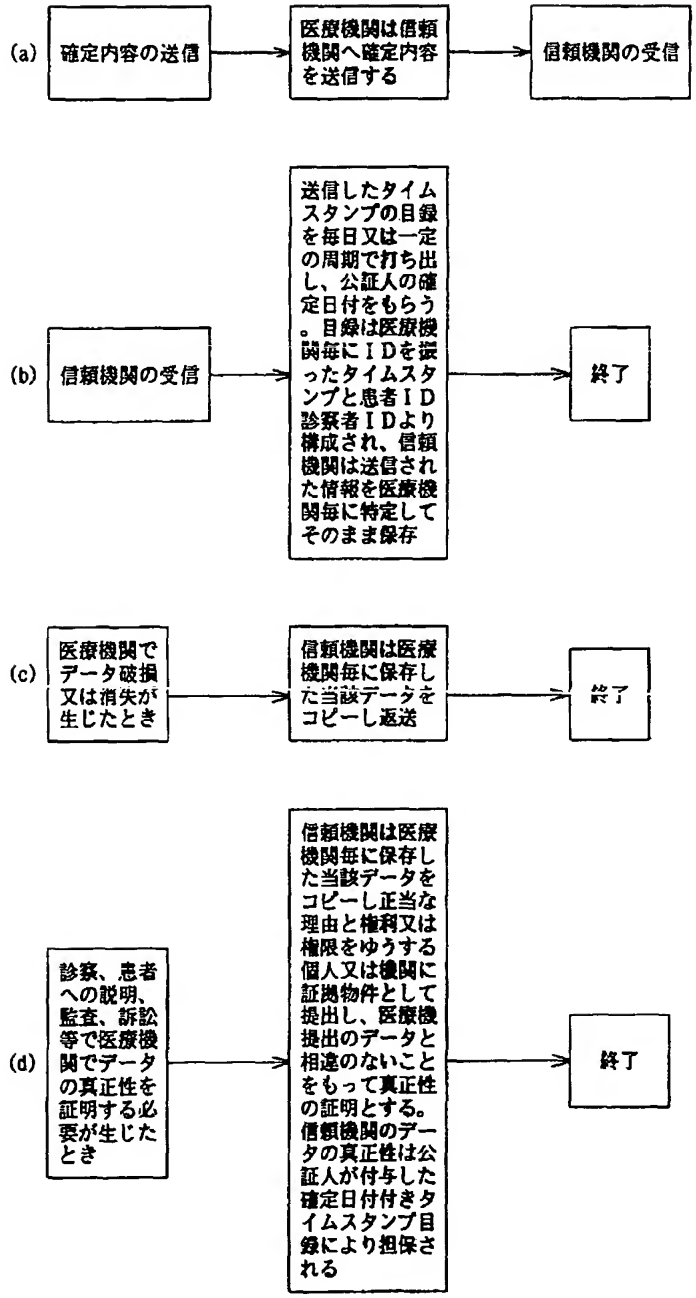
【図2】


1 患者は受診する
2－1 医師は一人の患者を診察する
2－2 医師又は入力者は頭書を入力、又は確認する
3 医師又は入力者は日々の画面に診療結果と検査、処方、病名等を入力する
4 患者に説明する
5－1 患者又はその家族等からインフォームドコンセントを得るか？
NO
YES
7 入力者識別入力
8 確定処理
6 年月日時と患者（又はＩＤ）又は家族等の名前を音声又は手書きで当該者に電子記録（患者サイン情報とする）してもらう
YES
NO
5－3 患者又は、その家族はカルテを閲覧することを同意するか？説明した内容を理解したことを確認する
5－2 医師は患者又はその家族に診察内容等の説明を行い、カルテを閲覧してもよい第三者（機関　職種　特定者）と閲覧してよい内容（医師診察所見　検査、処方、病名等）を説明する

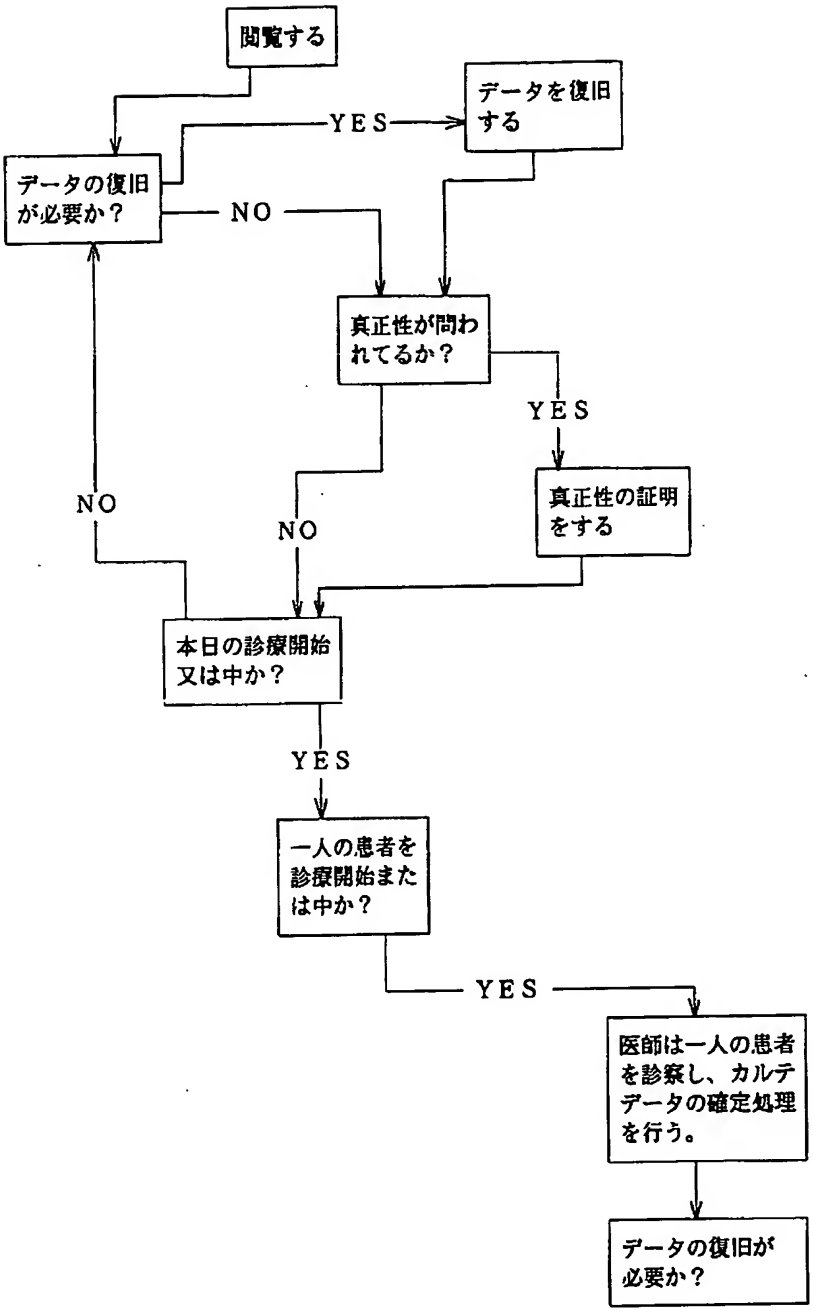
【図3】


確定処理
信頼機関からタイムスタンプをもらうか？
NO
YES
パスワードだけでよいか？
*
YES
NO
システムは入力者に漏洩を虚偽入力、書き換え、消去、混同対策のレベルを問い合わせる
手書きをもとめるか？
YES
NO
軽度の対策
YES
NO
信頼機関から暗号化しないタイムスタンプを得る
*
中程度の対策
YES
NO
信頼機関から共通鍵で暗号化したタイムスタンプを得る
*
高度の対策
信頼機関から公開鍵暗号方式を用い暗号化したタイムスタンプを得る
*
音声をもとめるか？
YES
NO
年月日時と診察者は入力者の名前（又はＩＤ）を音声で電子記録してもらう
その他の識別情報の取得
パスワード入力をもっ内れカルテ得られて容に得パスワード識加可処任者資報を付加不更変確定しとする等情しに理
システムは入力者に保存と漏洩虚偽入力、書き換え、消去、混同対策のレベルを問い合わせる
軽度の対策か？
YES
NO
信頼機関に暗号化しないタイムスタンプをもとめる
中程度の対策か？
YES
NO
共通鍵で暗号化したタイムスタンプをもとめる
高度の対策
公開鍵暗号方式を用い合化した

【図4】


(a)
確定内容の送信
医療機関は信頼機関へ確定内容を送信する
信頼機関の受信
(b)
信頼機関の受信
送信したタイムスタンプの目録を毎日又は一定の周期で打ち出し、公証人の確定日付をもらう。目録は医療機関毎にＩＤを振ったタイムスタンプと患者ＩＤ診察者ＩＤより構成され、信頼機関は送信された情報を医療機関毎に特定してそのまま保存
終了
(c)
医療機関でデータ破損又は消失が生じたとき
信頼機関は医療機関毎に保存した当該データをコピーし返送
終了
(d)
診察、患者への説明、監査、訴訟等で医療機関でデータの真正性を証明する必要が生じたとき
信頼機関は医療機関毎に保存した当該データをコピーし正当な理由と権利又は権限をゆうする個人又は機関に証拠物件として提出し、医療機提出のデータと相違のないことをもって真正性の証明とする。信頼機関のデータの真正性は公証人が付与した確定日付きタイムスタンプ目録により担保される
終了

【図5】


閲覧する
データを復旧する
YES
データの復旧が必要か？
NO
真正性が問われてるか？
YES
真正性の証明をする
NO
NO
本日の診療開始又は中か？
YES
一人の患者を診療開始または中か？
YES
医師は一人の患者を診察し、カルテデータの確定処理を行う。
データの復旧が必要か？